REMARKS

Claims 1-3, 6-12, 15-21 and 24-27 stand rejected under 35 USC §102(e) as anticipated by Schertz (U.S. 2003/0084322). Applicant respectfully disagrees with such rejection, particularly in view of the amendment made hereinabove.

In response to applicant's earlier amendments and arguments, the Examiner continues to rely on the excerpt from Schertz below to meet applicant's claimed "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (see this or similar, but not necessarily identical language in each of the independent claims).

> "[0021] ... Network-based intrusion protection systems deployed on dedicated appliances 80 and 81 are disposed on two sides of firewall/proxy server 60 to facilitate monitoring of attempted attacks against one or more nodes of network 100 and to facilitate recording successful attacks that successfully penetrate firewall/proxy server 60. Network intrusion protection devices 80 and 81 may respectively include (or alternatively be connected to) databases 80a and 81a containing known attack signatures. ..."
>
> [0023] ... Moreover, network intrusion protection devices 80 and 81 may be configured, for example by demand of IPS management node 85, to monitor one or more specific devices rather than all devices on a network. For example, network intrusion protection device 80 may be instructed to monitor only network data traffic addressed to web server 61. ..."
>
> [0030] ... In block 130, the OS-integrated intrusion detection system waits until a frame arrives. By examining the IP header, such as the identification field containing the IP datagram identifier, the flag field set to indicate more fragments, and the fragment offset field indicating the number of bytes the particular fragments is offset from the beginning of the datagram, a determination is made as to whether the received frame is a fragmented packet, as shown in block 132. If it is not a fragment, then the packet in the frame is compared to known intrusion signatures and viruses, as shown in block 134. If there is a match, then remedial or responsive action is taken, such as reporting to the system administrator, as shown in block 136. ..."

Applicant has carefully reviewed such excerpts and the remaining Schertz

references. However, it is clear that Schertz's pattern recognition is performed on a device-by-device basis or, in other words, at a "micro-level." In sharp contrast, applicant teaches and claims "detecting from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added), as claimed. Thus, contrary to the teachings of Schertz, applicant is capable of using data messages received from multiple networked computers at a managing computer for the purpose of detecting patterns across multiple computers. To this end, pattern detection may be extended to a network-wide scale, as opposed to the limited device-by-device manner of Schertz.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criteria has simply not been met by the Schertz reference. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has included the subject matter below in each of the independent claims.

> "applicant teaches and claims detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added)

No new matter has been added. Thus, it is now further emphasized that applicant teaches and claims detecting a network-wide threshold (in addition to patterns) across

multiple computers for detection of malware on a network-wide scale.

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P461/01.119.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100